Note that by the time we reach fields, we have added so many things to our rings that we may define a field in the following shorter way:

<u>Definition</u>: A <u>field</u> is a nonempty set F with two binary operations $\cdot$ and $+$ satisfying:

① $(F,+)$ and $(F^*,\cdot)$ are abelian groups.

② $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a,b,c \in F$.

Here, $F^* = F\setminus\{0\}$, because we don't want to ask for 0 (the identity in $(F,+)$) to have a multiplicative inverse.

<u>Example</u>: (A ring without unity which is non commutative)

Let $R = \left\{ A \in M_2(\mathbb{R}) \mid A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \text{ for some } a,b \right\}$.

Then we check:

<u>Claim</u>: $(R,+)$ is an abelian group (here, $+$ is matrix addition). First, R is closed w.r.t $+$, and:

① The operation $+$ is commutative

② Associative

③ Identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$.

(4) If $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \in R$, then the inverse $\begin{bmatrix} -a & -b \\ 0 & 0 \end{bmatrix} \in R$.

Next, observe that R is closed with respect to matrix multiplication, since

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}.$$ Then observe that

(5) Multiplication is associative, since matrix mult. is associative.

(6) Matrix multiplication distributes over matrix addition.

Last, note that R is <u>not</u> commutative since

$$\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ca & cb \\ 0 & 0 \end{bmatrix},$$ while

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}.$$

Also R does not have an identity, since

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} \Rightarrow a = 1$$

and $$\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} ca & cb \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$$

$\Rightarrow a=1$ and $cb=d \Rightarrow b=\frac{d}{c}$. In particular, for any matrix of the form

$$\begin{bmatrix} 0 & d \\ 0 & 0 \end{bmatrix}$$

the equation

$$\begin{bmatrix} 0 & d \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & d \\ 0 & 0 \end{bmatrix}$$ is impossible.

Example: A non-commutative ring with unity which is not a division ring.

~~Set~~ Consider $M_2(\mathbb{R})$, the set of all 2×2 matrices, with the operations of matrix addition and matrix multiplication.

We saw long ago that $(M_2(\mathbb{R}),+)$ is an abelian group, so ①-④ hold. Moreover, matrix multiplication is associative and distributes over addition, so $M_2(\mathbb{R})$ is a ring.

It has an identity: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and not every matrix is invertible. Moreover matrix multiplication is non-commutative.

Example: A commutative ring without identity.

Consider the even integers $2\mathbb{Z}$, with the usual addition and multiplication of integers. Then $(2\mathbb{Z},+)$ is an abelian group, so ①-④ are satisfied, so is associativity and distributivity of multiplication. So $2\mathbb{Z}$ is a ring.

Multiplication is clearly commutative, and there is no identity since $r\in 2\mathbb{Z} \Rightarrow rs>s$ or $rs<s$ for all $s\in 2\mathbb{Z}$, depending on the signs of r and s.

Example: A commutative ring with unity that is not an integral domain.

Consider $\mathbb{Z}_{12}$ with addition and multiplication mod 12. It is easy to see that this is a ring, moreover it is commutative and

$$1 \cdot r = r \cdot 1 = r \mod 12 \text{ for all } r.$$

So it has an identity as well. Yet we have

$$3 \cdot 4 \equiv 0 \mod 12$$

and neither 3 nor 4 is zero itself. Thus $\mathbb{Z}_{12}$ is not an integral domain.

Remark: A nonzero element a in a ring R is called a zero divisor if there exists $b \in R$ such that $ab = 0$, where $b \neq 0$. For example, 3 and 4 are both zero divisors in $\mathbb{Z}_{12}$.

Example: A division ring with non-commutative multiplication.

Let

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \underline{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad k = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

where $i^2 = -1$ and $\underline{i}$ is used to denote the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Let $\mathbb{H} \subseteq M_2(\mathbb{C})$ consist of all 2×2 matrices with complex entries that can be written as

$$a\cdot 1 + b\underline{i} + cj + dk \quad \text{for } a,b,c,d \in \mathbb{R}.$$

The ring operations are matrix addition and multiplication. The set $\mathbb{H}$ is obviously closed with respecto to addition and contains

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0\cdot 1 + 0\cdot \underline{i} + 0\cdot j + 0\cdot k,$$

so $(\mathbb{H},+)$ becomes an abelian group in the obvious way.

To see that $\mathbb{H}$ is closed with respect to matrix multiplication, note that any product of $\underline{i}, j, k, 1$ with any of $1, \underline{i}, j, k$ is again equal to an element of $\{1, \underline{i}, j, k\}$:

$$\underline{i}^2 = j^2 = k^2 = -1,$$

$$\underline{i}j = k$$

$$jk = \underline{i}$$

$$k\underline{i} = j$$

$$j\underline{i} = -k$$

$$kj = -\underline{i}$$

$$\underline{i}k = -j.$$

So the product of two elements of $\mathbb{H}$ is again in $\mathbb{H}$. (See text page 190 for a multiplication formula).

As usual, matrix multiplication is associative and distributes over +, so $\mathbb{H}$ is a ring.

In fact, $\mathbb{H}$ is a ring with identity since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}$.

Moreover, $\mathbb{H}$ contains all inverses of elements of $\mathbb{H}$:

One can check that

$$(a\cdot \mathbb{1} + b\cdot \underline{i} + c\cdot j + dk) \underbrace{\frac{1}{a^2+b^2+c^2+d^2}(a\cdot \mathbb{1} - b\cdot \underline{i} - c\cdot j - dk)}_{\text{So this is the inverse of } (a\cdot \mathbb{1} + b\cdot \underline{i} + c\cdot j + dk).} = \mathbb{1}$$

and

$$\frac{1}{a^2+b^2+c^2+d^2}(a\cdot \mathbb{1} - b\cdot \underline{i} - cj - dk)(a\cdot \mathbb{1} + b\underline{i} + cj + dk) = \mathbb{1} \checkmark.$$

Last, $\mathbb{H}$ is obviously not commutative, since

$\underline{i}j = k$ and $j\underline{i} = -k$, for example.

Thus $\mathbb{H}$ is a non-commutative ring with identity and inverses, so $\mathbb{H}$ is a division ring.

$\mathbb{H}$ is called the <u>quaternions</u>.

<u>Example</u>: An integral domain that is not a field.

Consider $\mathbb{Z}$ with its usual operations. As in the case of $2\mathbb{Z}$, it is a commutative ring. However $1 \in \mathbb{Z}$, so it is a commutative ring with identity. Moreover, in $\mathbb{Z}$ we know that $ab = 0$ implies either $a = 0$ or $b = 0$, so $\mathbb{Z}$ has no zero divisors. Thus it is an integral domain. Last, observe that $\mathbb{Z}$ is not a field: 2 does not have an inverse, for example.

<u>Example</u>: Fields.

With their usual operations, all of $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ are fields. There are also some less familiar fields, for example $\mathbb{Z}_p$ is a field when equipped with the usual $+$ and $\cdot$ mod p, and p is prime.

We already saw (in the case of $\mathbb{Z}_{12}$) that it's a commutative ring with 1. We only need to see that p prime $\Rightarrow$ every element has a multiplicative inverse.

Since p is prime, it is relatively prime to all $a \in \mathbb{Z}_p$, so $\exists\, x, y$ with

$$ax + py = 1$$

so that $ax \equiv 1 \mod p$.

But then $x = a^{-1}$, so $\mathbb{Z}_p$ is a field.

<u>Remark:</u> If every element has a multiplicative inverse, then there are no zero divisors!

Suppose not, say $ab = 0$ with neither a nor b zero, yet a^{-1} exists.

Then

$$a^{-1}(ab) = a^{-1} \cdot 0$$

$$\Rightarrow 1 \cdot b = 0$$

$$\Rightarrow b = 0.$$

<u>Note:</u> In the proof above we used $a^{-1} \cdot 0 = 0$. Why is this true?

<u>Proposition:</u> Let R be a ring and $a, b \in R$. Then:

① $a0 = 0a = 0$ for all $a \in R$

② $a(-b) = \overset{-ab}{\cancel{(-b)a}} = -ab$

③ $(-a)(-b) = ab$.

<u>Proof</u> ① Observe that $0 + 0 = 0$, so that

$$a0 = a(0+0) = a0 + a0$$

so cancelation gives $a0 = 0$. Similarly $0a = 0$.

② Observe that

$$ab + a(-b) = a(b-b) = a0 = 0$$

so that $a(-b) = -ab$.

Similarly we show $\cancel{(-b)a} = -ab = (-a)b$

③ We can prove ③ using ②, since

$$\underbrace{(-a)(-b) = -(a(-b))}_{\text{using } (-a)b=-ab \text{, replacing } b \text{ with } -b} = \underbrace{-(-ab)}_{\text{using } (g^{-1})^{-1}=g} = ab$$

using ② again.

using $(-a)b = -ab$, replacing b with $-b$

using $(g^{-1})^{-1} = g$, something we proved for all groups.

Therefore we can use our familiar algebraic rules for manipulating elements of rings.

Just as in the case of groups, where a subset $H \subset G$ can inherit the binary operation from G and become a group, the same is true of rings.

Definition: Let R be a ring. A subset $S \subset R$ is a subring if, when equipped with the operations $+$ and $\cdot$ from R, S becomes a ring.

As in the case of groups, we have a proposition that makes checking easier:

Proposition: Let R be a ring and $S \subset R$ a subset. Then S is a subring of R if and only if the following hold:

① $S \neq \emptyset$

② $rs \in S$ for all $r, s \in S$

③ $r - s \in S$ for all $r, s \in S$.

If R has identity 1_R and S has identity 1_S, then $1_R = 1_S$.

Proof: If S is a subring then these properties obviously hold. On the other hand, if S satisfies ① – ③ then we show that S is a ring as follows:

By an earlier proposition, ① and ③ imply that $(S,+)$ is an abelian group, So S satisfies properties ①–④ of the definition of a ring. Property ⑤ (associativity) holds because multiplication in R is associative since R is a ring. Similarly, ⑥ holds because distributivity holds in R (thus in S).

Examples: If we consider easy examples first:

$$n\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

are all subrings, and this is straightforward to check. A less straightforward example:

Let $R = M_2(\mathbb{R})$ and let

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a,b,c \in \mathbb{R} \right\}.$$

We check that S is a subring:

First, S is nonempty, and if $A, B \in S$, say

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \quad B = \begin{pmatrix} r & s \\ 0 & t \end{pmatrix}, \text{ then}$$

$$AB = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} r & s \\ 0 & t \end{pmatrix} = \begin{pmatrix} ar & as+bt \\ 0 & ct \end{pmatrix} \in S;$$

and

$$A - B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} = \begin{pmatrix} a-r & b-s \\ 0 & c-t \end{pmatrix} \in S.$$

So S is a subring by our proposition.

Sometimes subrings have different properties than the larger ring. For example, a subgroup $H \subset G$ can be abelian even though G is not abelian.

Example: Consider the field $\mathbb{C}$, and the subset

$$\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$$

Then $\mathbb{Z}[i]$ is a subring since it is nonempty and is closed under multiplication:

$$(a+bi)(c+di) = (ac-bd) + (bc+ad)i$$

$$ac-bd,\ bc+ad \in \mathbb{Z}$$

and also under addition:

$$(a+bi)+(c+di) = (a+c) + (b+d)i, \quad a+c,\ b+d \in \mathbb{Z}.$$

This ring is called the Gaussian integers. However, $\mathbb{Z}[i]$ is not a field (even though it is a subring of a field), because elements do not have multiplicative inverses.

In fact, we can determine all elements in $\mathbb{Z}[i]$ that have inverses as follows:

Suppose $a+bi=\alpha$ has an inverse β. Then $\bar{\alpha}=a-bi$ has an inverse too, since $\alpha\beta=1$
$$\Rightarrow \bar{\alpha}\bar{\beta}=1.$$

Writing $\beta=c+di$, we calculate
$$1=\alpha\beta\bar{\alpha}\bar{\beta}=\alpha\bar{\alpha}\beta\bar{\beta}=(a^2+b^2)(c^2+d^2),$$
so $a^2+b^2=\pm 1$ (since we're working with integers). Therefore $a+bi=\pm i$ or $a+bi=\pm 1$. So the only elements in $\mathbb{Z}[i]$ with multiplicative inverses are $\pm i, \pm 1$.

<u>Definition</u>: An element $a \in R$ is called a <u>unit</u> if it has a multiplicative inverse.

<u>Example</u>: We saw that $R=GL_2(\mathbb{R})$ is a ring. This is also true if we take $R=GL_2(\mathbb{Z}_2)$, the set of 2×2 matrices with entries in $\mathbb{Z}_2$. However, $GL_2(\mathbb{Z})$ is not a field (since some matrices are not invertible, like $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$).

In fact $GL_2(\mathbb{Z})$ is not even a division algebra.

$GL_2(\mathbb{Z})$ is also not an integral domain, since

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

However, let $F \subset GL_2(\mathbb{Z})$ be the set

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Then F is a subring (check this!) and in fact F is also a field.

__Remark__: The previous two examples show that by passing to a subring we may either "lose some structure", as in example 1

or

"gain some structure", as in example 2.

__Proposition__: (Multiplicative cancelation)
Let R be a commutative ring with identity. Then R is an integral domain if and only if for all nonzero elements $a \in R$, $ac = ab \Rightarrow c = b$.

__Proof__: Suppose R is an integral domain, and $a \neq 0$. Then $ac = ab \Rightarrow a(c-b) = 0$, since R has no zero divisors thus forces $c-b=0 \Rightarrow b=c$.

Conversely suppose that for all $a \neq 0$, $ab=ac \Rightarrow b=c$. Suppose $ax=0$ and $a\neq 0$. Then $ax=0$ can be rewritten as $ax=a\cdot 0$, forcing $x=0$. So a is not a zero divisor, and R is an integral domain.

<u>Theorem (Wedderburn)</u>:

Every finite integral domain is a field.

<u>Proof</u>: Suppose D is a finite integral domain, and let $D^* = D\setminus\{0\}$. We must show that every $a\in D^*$ has an inverse. For each such a, define a map $\lambda_a : D^* \longrightarrow D^*$ by $\lambda_a(d) = ad$.

Note that the image of this map is contained in D^* as claimed, since $a\in D^*$ and $d\in D^*$ $\Rightarrow ad \neq 0$, since D has no zero divisors.

The map is also 1-to-1, since

$$\lambda_a(d) = \lambda_a(d')$$
$$\Rightarrow ad = ad'$$
$$\Rightarrow d=d', \text{ since we're in an integral domain.}$$

Since D^* is a finite set, this means the map λ_a must also be onto, in particular $\exists d \in D^*$ with $\lambda_a(d) = 1$. But $ad = 1$ means a has an inverse (recall D is commutative) and therefore $\underline{\underline{D \text{ is a field}}}$.

For any nonnegative integer n and $r \in R$ an element of any ring, we'll abbreviate

$$\underbrace{r+r+\ldots+r}_{n \text{ times}} \quad \text{as} \quad nr.$$

<u>Definition</u>: The <u>characteristic</u> of a ring R is the smallest integer n, $(n>0)$ such that $nr=0$ for all $r \in R$. If no such n exists, we say that R has characteristic zero.

<u>Example</u>: The field $\mathbb{Z}_p$ has characteristic p, since $pr \equiv 0 \bmod p$ for all $r \in \mathbb{Z}_p$.

In general, determining the characteristic of a ring can be tough, so we have a lemma to help:

<u>Lemma</u>: Let R be a ring with identity. If 1 has order n in the abelian group $(R,+)$, then the characteristic of R is n.

<u>Proof</u>: If $n \cdot 1 = 0$, then for all $r \in R$ we have

$$n \cdot r = n \cdot 1 r = (n \cdot 1) r = 0 \cdot r = 0.$$

On the other hand, if no such n exists then R has characteristic zero.

This allows us to prove:

<u>Theorem</u>: The characteristic of an integral domain is either prime or zero.

<u>Proof</u>: Let D be an integral domain, and suppose that the characteristic of D is n, $n \neq 0$. Suppose n is not prime, and write $n = ab$ with $0 < a < n$ and $0 < b < n$. Then:

$$0 = n \cdot 1 = ab \cdot 1 = (a \cdot 1)(b \cdot 1)$$

$$\Rightarrow a \cdot 1 = 0 \text{ or } b \cdot 1 = 0, \text{ since } D \text{ is an integral domain.}$$

However neither $a \cdot 1 = 0$ nor $b \cdot 1 = 0$ is possible, since R would then have characteristic less than n, by our lemma. Therefore n must be prime.

§ 16.3 Ring homomorphisms, ideals and quotients.

In our study of groups, we saw that a group homomorphism is a map

$$\phi : G \longrightarrow H$$

that respects the group operation. We also saw that

$$\ker \phi = \{ g \in G \mid \phi(g) = e \}$$

is a normal subgroup, and in fact any normal subgroup $N \subset G$ is the kernel of a homomorphism

$$\phi : G \longrightarrow G/N \qquad \phi(g) = gN$$

(The kernel is exactly $g \in G$ s.t. $gN = N$, ie. it's N)

The same is true for rings. We have ring homomorphisms kernels and quotients all related the same way.

<u>Definition</u>: A ring homomorphism $\phi : R \longrightarrow S$ is a map between rings R and S satisfying

$$\phi(a+b) = \phi(a) + \phi(b)$$

$$\text{and } \phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in R$. If ϕ is bijective then it is called an <u>isomorphism</u> of rings.

Example: Define $\phi: \mathbb{Z} \to \mathbb{Z}_n$ (n any integer) by $\phi(a) = a \bmod n$. It's a ring homomorphism because

$$\begin{aligned}\phi(a+b) &= a+b \bmod n \\ &= a \bmod n + b \bmod n \\ &= \phi(a) + \phi(b)\end{aligned}$$

and

$$\begin{aligned}\phi(ab) &= ab \bmod n \\ &= (a \bmod n)\cdot(b \bmod n) \\ &= \phi(a)\phi(b).\end{aligned}$$

Thus ϕ is a homomorphism.

Example: Let $C[a,b]$ denote the set of continuous functions $f: [a,b] \longrightarrow \mathbb{R}$. Then $C[a,b]$ is a ring because

- the sum of continuous functions is continuous, and if f is continuous so is $-f$.
- the product of continuous functions is continuous.

Fix a number $x_0 \in [a,b]$, and define a map

$$\phi_{x_0}: C[a,b] \longrightarrow \mathbb{R} \text{ by}$$

$$\phi_{x_0}(f) = f(x_0) \quad \text{(evaluate the function at } x_0\text{)}$$

Then ϕ_{x_0} is a ring homomorphism since

$$\phi_{x_0}(f+g) = (f+g)(x_0) = f(x_0) + g(x_0)$$
$$= \phi_{x_0}(f) + \phi_{x_0}(g).$$

and $\phi_{x_0}(f \cdot g) = (f \cdot g)(x_0) = f(x_0)\,g(x_0)$

$$= \phi_{x_0}(f)\,\phi_{x_0}(g).$$

function multiplication, like $f(x)g(x)$, <u>not</u> composition!

This is called an <u>evaluation</u> <u>homomorphism</u>.

<u>Definition</u>: The <u>kernel</u> of a ring homomorphism $\phi: R \longrightarrow S$ is the set

$$\ker \phi = \{ r \in R \mid \phi(r) = 0 \}.$$

<u>Example</u>: For our first homomorphism $\phi: \mathbb{Z} \to \mathbb{Z}_n$, the kernel is

$$\ker \phi = \{ m \in \mathbb{Z} \mid \phi(m) = 0 \}$$
$$= \{ m \in \mathbb{Z} \mid m \equiv 0 \bmod n \}$$
$$= n\mathbb{Z}.$$

For our second homomorphism $\phi_{x_0}: C[a,b] \longrightarrow \mathbb{R}$, the kernel is

$$\ker \phi = \{ f \in C[a,b] \mid \phi_{x_0}(f) = 0 \}$$
$$= \{ f \in C[a,b] \mid f(x_0) = 0 \}$$
= functions $f : [a,b] \longrightarrow [a,b]$ that are continuous and have a root at x_0.

<u>Proposition</u>: Let $\phi : R \longrightarrow S$ be a ring homomorphism. Then

① If R is a commutative ring, then $\phi(R)$ is a commutative ring ($\phi(R)$ is always a subring)

② $\phi(0) = 0$

③ If R and S have identities 1_R and 1_S, then $\phi(1_R) = 1_S$ <u>provided</u> <u>ϕ is onto</u>!

④ If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.

<u>Proof</u>: We leave ① and ④ as exercises. To prove ②, note that if $\phi : R \longrightarrow S$ is a ring homomorphism, then $\phi : (R, +) \longrightarrow (S, +)$ is a homomorphism of abelian groups. Since group homomorphisms send identities to identities,

$$\phi(0) = 0.$$

To prove 3, choose an element $a \in R$ with $\phi(a) = 1_S$.

The we compute:

$$\begin{aligned}
&\phi(1_R) - 1_S \\
&= \phi(1_R) - \phi(a) \\
&= (\phi(1_R) - \phi(a))\phi(a) \qquad (\text{since } \phi(a) = 1_S) \\
&= \phi(1_R)\phi(a) - \phi(a) \qquad (\text{since } (\phi(a))^2 = \phi(a)) \\
&= \phi(1_R \cdot a) - \phi(a) \\
&= \phi(a) - \phi(a) = 0.
\end{aligned}$$

So $\phi(1_R) = 1_S$.

<u>Example</u>: Consider the map $\phi : \mathbb{Z} \longrightarrow M_2(\mathbb{R})$ given by $\phi(n) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$. The map ϕ is a homomorphism because

$$\phi(n+m) = \begin{pmatrix} n+m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \phi(n) + \phi(m),$$

and

$$\phi(nm) = \begin{pmatrix} nm & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \phi(n)\phi(m)$$

However, the identity in $M_2(\mathbb{R})$ is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, whereas the identity in $\mathbb{Z}$ is 1 and

$$\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

So in part ③ of the previous theorem, <u>onto</u> is required.

Now we'll define quotients of rings. When studying groups, we defined quotients by first studying normal subgroups $N \subset G$. Then G/N is a set of cosets, with a group operation.

In the case of rings, normal subgroups will be replaced by special subrings called <u>ideals</u>; and when $I \subset R$ is an ideal we will take a quotient R/I. The quotient R/I will be a set of cosets as before, with ring operations defined using the operations from R.

<u>Notation:</u> If $S \subset R$ is a subring and $r \in R$, set $rS = \{rs \mid s \in S\}$ and $Sr = \{sr \mid s \in S\}$. Recall that we already have a notation

$r + S = \{r + s \mid s \in S\}$ for the cosets of $S \subset R$, considering both S and R as abelian groups.

Definition: An ideal in a ring R is a subring $I \subset R$ satisfying:

If $a \in I$ and $r \in R$, then $ar \in I$ and $ra \in I$

In other words, $rI \subset I$ and $Ir \subset I$.

Example: Every ring has two ideals (at least), namely $\{0\}$ and the whole ring.

Example: Let R be a commutative ring with identity, and choose $a \in R$. Set

$$\langle a \rangle = \{ar \mid r \in R\}.$$

Claim: $\langle a \rangle$ is an ideal.

First we check $\langle a \rangle$ is a subring. Note $\langle a \rangle \neq \emptyset$, since $a \cdot 0 = 0 \in \langle a \rangle$. Note also that if $ar, as \in \langle a \rangle$ then $ar - as = a(r-s) \in \langle a \rangle$. So $\langle a \rangle$ is a subgroup of $(R, +)$. Last, if $ar, as \in \langle a \rangle$ then

$$ar \cdot as = a(ars) \in \langle a \rangle,$$

so $\langle a \rangle$ is a subring. Finally, it is an ideal since for any $r' \in R$,

$$\begin{aligned} r'\langle a \rangle &= \{r'ar \mid r \in R\} \\ &= \{ar'r \mid r \in R\} \subset \langle a \rangle \end{aligned}$$

and similarly $\langle a \rangle r' \subset \langle a \rangle$. The ideal $\langle a \rangle$ is called the <u>principal</u> <u>ideal</u> generated by a.

<u>Example</u>: Consider the ring $R = \mathbb{Z}$. It has plenty of ideals, namely

$$\langle n \rangle = n\mathbb{Z} \subset \mathbb{Z} \quad \text{for all } n.$$

<u>Theorem</u>: Every ideal in $\mathbb{Z}$ is of the form $\langle n \rangle$ for some $\langle n \rangle \subset \mathbb{Z}$.

<u>Proof</u>: Let $I \subset \mathbb{Z}$ be an ideal. If $I = \{0\}$ then $I = \langle 0 \rangle$, so the claim holds when I is the trivial ideal.

If $I \neq \{0\}$, then I contains a positive integer m, by the well-ordering principle I contains some least positive integer, say n.

Now let $a \in I$ be given, and write

$$a = nq + r \quad \text{using the division algorithm,}$$
$$\text{so} \quad 0 \leq r < n.$$

But then $r = a - nq$, and $a \in I$, $nq \in I$ (since I is an ideal) implies $r \in I$. This forces $r = 0$ since n is minimal. Therefore $a = nq$ and $I = \langle n \rangle$.

<u>Example</u>: Let $\phi : R \to S$ be a ring homomorphism. Then $\ker\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R, here's why:

First, $\ker\phi$ is a subring because:

① $0 \in \ker\phi$

② If $r, s \in \ker\phi$ then $\phi(r-s) = \phi(r) - \phi(s) = 0 - 0 = 0$, so $r - s \in \ker\phi$

③ If $r, s \in \ker\phi$ then $\phi(rs) = \phi(r)\phi(s) = 0 \cdot 0 = 0$.

Next, $\ker\phi$ is an ideal because if $r \in R$ then $s \in \ker\phi$ implies

$$\phi(rs) = \phi(r)\phi(s) = \phi(r) \cdot 0 = 0, \text{ so } rs \in \ker\phi$$

$$\phi(sr) = \phi(s)\phi(r) = 0 \cdot \phi(r) = 0, \text{ so } sr \in \ker\phi.$$

Thus $\ker\phi$ is an ideal.

<u>Remark</u>: Something we will largely avoid in this course is the following subtle point: Since a ring R may not have a commutative multiplication, it's possible that $rI \neq Ir$. If this happens, then you can have

$$rI \subset I \quad \underline{\text{but not}} \quad Ir \subset I \qquad ①$$

or

$$Ir \subset I \quad \underline{\text{but not}} \quad rI \subset I. \qquad ②$$

Some books track this subtle point carefully by calling subrings satisfying ① left ideals, and subrings satisfying ② right ideals.

Then a subring I with $rI \subset I$ and $Ir \subset I$ (for us, an ideal) is called a two-sided ideal.

Beware of these distinctions when reading supplementary material!

Definition: Let R be a ring, and $I \subset R$ an ideal. Then the set of cosets R/I is an abelian group with operation

$$(r+I)+(s+I) = (r+s)+I,$$

as we saw in Chapter 10. However R/I is in fact a quotient ring, with multiplication of cosets defined by

$$(r+I)(s+I) = rs+I.$$

Theorem: The set of cosets R/I with the operation above gives R/I the structure of a ring.

Proof: From our discussion of quotient groups, ~~we~~ we already know that R/I with addition defined as above is an abelian group.

So, we only need to study multiplication on R/I.
First we check the multiplication is well-defined, so suppose $r+I = r'+I$ and $s+I = s'+I$. Then in particular $r' \in r+I$ and $s' \in s+I$, so there exist elements $a, b \in I$ such that

$$r' = r+a \quad \text{and} \quad s' = s+b.$$

Then we compute

$$r's' = (r+a)(s+b) = rs + \underbrace{\underset{rI}{\underset{\cap}{rb}} + \underset{Is}{\underset{\cap}{as}} + \underset{I}{\underset{\cap}{ab}}}_{\substack{\text{since } I \text{ is an ideal, this} \\ \text{part is contained in } I}} \in rs + I.$$

Therefore $r's' \in rs+I$. From our work with groups, we know that this implies $r's'+I = rs+I$. Therefore

$$(r+I)(s+I) = (r'+I)(s'+I).$$

The associative law for multiplication in R/I holds because multiplication in R is associative. Last, we check:

$$\begin{aligned}
&(r+I)\big((a+I)+(b+I)\big) \\
&= (r+I)\big((a+b)+I\big) = r(a+b)+I \\
&\qquad\qquad\qquad\qquad\quad = (ra+rb)+I \\
&\qquad\qquad\qquad\qquad\quad = ra+I + rb+I \\
&\qquad\qquad\qquad\qquad\quad = (r+I)(a+I) + (r+I)(b+I)
\end{aligned}$$

so the operation distributes over $+$ from the left. Distributivity from the right is similar.

<u>Example</u>: We saw already that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n \quad \underline{\text{as groups}},$$

but in fact $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ as <u>rings</u>, since $\mathbb{Z}_n$ has both addition and multiplication operations inherited from $\mathbb{Z}$.